BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Operațiile de informații, proiecte de rivalitate în Arena informațiilor

Information operations, rivalry projects in the information arena

Lect.univ.Dr. Cristinel-Marius AMZA*
*Universitatea Națională de Apărare „Carol I", București
e-mail: amza.marius@unap.ro

Abstract

Organizarea și desfășurarea operațiilor de informații în Arena informațiilor implică o rivalitate și o confruntare reală între serviciile de informații, pentru a câștiga unele avantaje în defavoarea celorlalte. Nu este deloc surprinzător faptul că acești rivali încearcă permanent, pe de-o parte, să-și împiedice reciproc eforturile de a se cunoaște unul pe celălalt, și, pe altă parte, să-l inducă în eroare, să-l dezinformeze sau să-l înșele.

The organization and conduct of intelligence operations in the Intelligence Arena involves a real rivalry and confrontation among the Intelligence Services, conducted in order to gain some advantages at the expense of others. Nothing is surprising in the fact that these rivals are constantly trying on the one hand to thwart each other's efforts to know the other, and, on the other hand, to mislead, misinform, or deceive.

Cuvinte-cheie:
operații de informații; factori de decizie; ISR; contrainformații; clandestin; secret.

Keywords:
intelligence operations; ISR; counterintelligence; clandestine; confidential; secret.

Info articol
Primit: 2 octombrie 2024; Evaluat: 1 noiembrie 2024; Acceptat: 13 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Amza, C.M. 2024. „Operațiile de informații, proiecte de rivalitate în Arena informațiilor".
Buletinul Universității Naționale de Apărare „Carol I", 13(4): 168-181. https://doi.org/10.53477/2065-8281-24-46

La acest moment, putem afirma că majoritatea strategiilor de securitate sau de apărare, elaborate de cele mai multe state ale lumii fac referire, în speță, la interesele naţionale, iar acestea sunt cele care determină acţiunile acestora pe scena internaţională, asigurându-se că supravieţuiesc.
Culegerea de informații referitoare la adversari a fost și este esențială pentru elaborarea acestor strategii militare încă de la apariția rivalităților. Cunoașterea capacităților adversarilor, a ordinii de luptă și a intenției poate face diferența dintre victorie și înfrângere. Fie prin intermediul senzorilor umani și interceptarea comunicațiilor, fie prin observarea de pe vârful unui deal sau, în epoca modernă, de la cel mai înalt nivel al spațiului, abilitatea de a cunoaște ceea ce face adversarul este esențială pentru înțelegere și, în cele din urmă, pentru victorie.
În contextul mediului actual de securitate, dependența puterii naționale de sfera informațiilor este evidentă și impune ca structurile de informații să fie capabile să sprijine politica externă dorită de factorii de decizie de la nivelul strategic. Statele dominante creează și își configurează serviciile de informații pentru a-și spori puterea în relațiile internaționale, iar din această perspectivă, acestea sunt, în esență, „arene de acțiune pentru relațiile de putere" (Morgenthau 2007; Evans și Wilson 1992, 330).

Informațiile înseamnă cunoașterea mediului de securitate, a actorilor și forțelor care reprezintă o amenințare la adresa unui stat (NATO AAP-6 2021). Cunoştinţele sunt în sprijinul factorului politic și militar care sunt parte componentă a procesului decizional și rezultatul culegerii, prelucrării, exploatării, integrării și interpretării informațiilor disponibile privind mediul actual de securitate și amenințările.
Informațiile au două mari obiective: primul este reducerea incertitudinii prin furnizarea de informații precise, oportune și relevante, a datelor referitoare la amenințări și mediul înconjurător, iar cel de-al doilea se referă la protejarea teritoriului național și a cetățenilor prin desfășurarea de activități și acțiuni de contrainformații.

Sfera intereselor și divergențele de geopolitică, geostrategie, economie și ideologie dintre actorii statali nu vor permite niciodată decidenților de la nivelul strategic să aibă o imagine clară asupra mediului de securitate, de aceea informațiile acoperă cel mai mare număr de necunoscute și trebuie să răspundă întrebărilor legate de acestea pentru cunoașterea adevăratelor intenții. Aproape întotdeauna vor exista lacune în informații și în datele furnizate și va lipsi gradul de detaliu dorit, deoarece informațiile nu pot oferi absolut totul cu certitudine, acestea utilizează probabilități, dar încearcă să reducă incertitudinea, înfruntându-l pe competitor prin culegerea de informații relevante, prin plasarea lor în context pentru a oferi cunoștințe și a le transmite pentru formarea imaginii complete și pentru a îmbunătăți înțelegerea acesteia, iar în acest sens, desfășurarea acțiunii de informații și de contrainformații de către serviciile de informații este relevantă.

O abordare a arenei informațiilor din punctul de vedere al operațiilor de informații constă în clasificarea acestora în trei mari categorii: prima categorie se referă la

culegerea de date și informații pentru procesarea, transformarea în produse finite de informații și diseminarea acestora către decidenți, cea de-a doua categorie se referă la acele operații de informații, întreprinse pentru a influența cursul unor evenimente, numite, uneori, operații clandestine sau secrete, iar cea de-a treia cuprinde operațiile de contrainformații, executate pentru a contracara operațiile de informații, indiferent de natura adversarului. Toate aceste trei tipuri de operații de informații vor avea impact asupra politicii externe a oricărui stat. Impactul va varia în ceea ce privește atât domeniul de aplicare, cât și gradul de implicare, pentru că factorul politic este cel care aprobă planificarea și executarea operațiilor de informații (Westwood 1977, 86).

O operație de informații este un proiect unic și complex, planificată și executată pe o perioadă de timp medie și îndelungată, cu resurse umane experimentate și cu un consum uriaș de resurse materiale și financiare pentru a îndeplini obiectivele. Un asemenea proiect constă într-un număr variabil de faze, subfaze, sarcini și acțiuni colective și individuale, executate într-o concepție unitară, iar realizarea este posibilă numai prin coordonarea și relaționarea de către un grup multidisciplinar, alcătuit din personal de informații (ofițeri operativi, analiști, personal tehnic, IT etc.), a fazelor, activităților și sarcinilor. Obiectivul principal al gestionării implementării proiectului operației este acela de a asigura performanța și calitatea tehnică necesară cu cel mai mic risc posibil și într-un timp cât mai rezonabil.

Operațiile de informații pentru culegerea de date și informații în scopul procesării și transformării acestora în produse finite de informații sunt necesare în acțiunile militare, deoarece aduc clarificarea mediului strategic, operațional și tactic, clarifică intențiile adversarului și sunt esențiale pentru deciziile comandantului. Informațiile includ organizațiile, capacitățile și procesele utilizate pentru sarcini, culegere, procesare, analiza și exploatarea informațiilor din mai multe surse, cu accent permanent pe satisfacerea cerințelor de informații ale comandantului grupării de forțe întrunire (JFC), iar acțiunile de informații se desfășoară în și din toate domeniile pe toată durata competiției (U.S. Air Force Doctrine 2023).
Informațiile le permit liderilor de la toate nivelurile să ia decizii pentru aplicarea puterii de luptă. Succesul în operații necesită decizii oportune și eficiente, bazate pe aplicarea logicii informațiilor și cunoștințelor disponibile. Prin urmare, comandanții și statele majore caută să construiască și să mențină înțelegerea permanentă a situației pe parcursul operației.

Operațiile de informații cuprind culegerea de informații din toate domeniile cu întregul spectru de capabilități al senzorilor, procesarea, exploatarea, analiza integrată și activități de furnizare de informații la nivel de mare unitate, centre de operații (aeriene, navale și terestre), distribuite beneficiarilor și centrelor naționale de producție. Aceste operații au ca rezultat diseminarea de informații către utilizatorii tactici, operaționali și strategici prin parcurgerea unui ciclu de informații: planificare și direcționare; culegere, procesare, analiză; diseminare; evaluare și feedback. Important este faptul că evaluarea și feedbackul sunt continue și facilitate pe tot parcursul ciclului prin colaborare și dialog cu toate părțile interesate.

Serviciile întrunite de informații, supraveghere și cercetare (JISR) sunt vitale pentru toate operațiile militare și oferă factorilor de decizie și statelor majore o mai bună cunoaștere a situației din mediul operațional. Pentru a permite culegerea informațiilor și pentru a se asigura că informațiile sunt analizate și sunt diseminate factorilor de decizie, există o serie de actori primari implicați, inclusiv mijloacele de culegere, supraveghere și cercetare (de exemplu, aeronavele de supraveghere Alliance Ground Surveillance și Airborne Warning & Control System, care utilizează radare, sateliți de observare, mijloace electronice și structuri de cercetare pentru a culege informații), analiștii de informații și factorii de decizie.

Cercetarea specială (special reconnaissance) reprezintă acțiunile de cercetare și supraveghere, efectuate ca o operație specială în medii ostile, greu accesibile sau sensibile din punct de vedere politic și/sau diplomatic pentru a culege sau a verifica informații de importanță strategică sau operațională, evitându-se descoperirea și lupta directă cu inamicul. Cercetarea specială se execută de subunități mici, cum ar fi un detașament sau o echipă de cercetare, formată din personal militar cu un nivel de pregătire ridicat, de obicei din unități de forțe speciale sau structuri de informații militare.

Ca scop și rol, cercetarea specială este diferită de acțiunile de comando, dar ambele sunt, de regulă, efectuate de aceleași tip de subunități. Rolul cercetării speciale include sprijinul direct al loviturilor operațiilor aeriene prin oferirea de imagini, permițând echipajelor să ajusteze atât strategia de zbor, cât și pe cele ale sistemelor de artilerie și de rachete terestre în zonele de operații din adâncimea dispozitivului inamicului, plasarea de senzori acționați și monitorizați de la distanță și pregătirile specifice pentru acțiunile altor structuri de forțe speciale sau informații militare. În multitudinea de misiuni pe care le pot executa subunitățile de cercetare specială, se regăsesc și acțiunile directe la obiective, precum și cele de război neconvențional, inclusiv operațiile de gherilă. Subunitățile de cercetare specială, pe lângă faptul că au un nivel înalt de pregătire, au și o echipare și dotare cu tehnică și armament calitativ superioară, deoarece trebuie să lupte în condiții dificile, adeseori cu un raport de forțe defavorabil, atunci când sunt descoperite, iar elementele de asigurare a extragerii vor avea nevoie de timp pentru a ajunge la ele.

În timpul primului Război din Golf din 1991, unitățile SAS britanice și forțelor aeriene ale SUA au fost trimise, inițial, în adâncimea dispozitivului de luptă irakian pentru a găsi lansatoarele de rachete Scud și pentru a direcționa loviturile executate de mijloacele aeriene. Atunci când acțiunile aeriene au întârziat, patrulele au atacat infrastructurile critice ale sistemelor Scud cu armamentul și cu tehnica din dotare.

În urma executării unei operații de cercetare specială, debriefingul structurilor poate fi făcut de ofițerii HUMINT, care sunt cel mai familiarizați cu tehnicile lor de culegere a informațiilor, deoarece este posibil ca informațiile rezultate să contribuie la culegerea informațiilor HUMINT, dar, în funcție de misiune, pot contribui și pentru IMINT, SIGINT, MASINT și TECHINT. Unele dintre aceste tehnici și proceduri sunt extrem de sensibile și confidențiale, fiind gestionate pe baza principiului „nevoii

de a cunoaște" în cadrul structurilor care coordonează operația de cercetare specială, inclusiv pentru membrii celulei de informații din toate sursele.

Operațiile de informații discrete, ascunse sau secrete ale unui guvern care urmărește influențarea evenimentelor în alte state nu sunt decât o mică parte a relațiilor internaționale, dar acestea există tocmai pentru a sprijini factorii de decizie. Planificarea și executarea acestui tip de operații au avantajul distinct al realizării politicii fără a pune în joc aspectul național și indiferent de natura lor, atunci când structurile de informații eșuează, nu lasă gustul amar al înfrângerii ca într-o confruntare.

Doctrina considerată multă vreme axiomatică, potrivit căreia șeful statului ar trebui să poată nega că a autorizat sau chiar că a avut cunoștință de o astfel de operațiune, chiar dacă implicarea unui stat într-o acțiune secretă devine cunoscută, este strâns legată de cele afirmate anterior. Acesta ar trebui să poată afirma, destul de plauzibil, că operația a fost îndeplinită de subordonații săi care au acționat fără știrea ori autorizarea lui (Shulski și Schmitt 2008, 151).

Operațiile de informații care urmăresc influențarea evenimentelor le putem clasifica în următoarele tipuri de operații: „discrete", „sub acoperire", „clandestine" și „sub steag fals". În acest articol, voi folosi termenul de operații „discrete" pentru a face diferența de operațiile „sub acoperire" și „clandestine".
O operație discretă (black operation) este o operație secretă a unei agenții guvernamentale, a unei entități militare sau a unei organizații paramilitare și poate include și activități ale entităților private, având ca obiectiv principal intrarea clandestină sau în secret în cadrul structurilor țintă ale unui competitor pentru a obține informații cu ajutorul surselor umane. Aceasta este în mod evident cea mai bună situație, în cazul culegerii de informații, din moment ce este dobândit accesul la documente secrete sau fragmente de informații, utile ori necesare. Caracteristicile de bază ale unei operații discrete constau în faptul că aceasta este confidențială și nu poate fi atribuită organizației care o desfășoară (Smith Jr. 2003). Acest tip de operație de informații a fost planificată și executată de majoritatea serviciilor specializate, precum MI6, MI5, Mossad, CIA, KGB, FSB, ISI, precum și de structuri de informații ale altor state (Intelnews 2008).

Diferența majoră dintre o operație discretă și una care este pur și simplu secretă este că o operație discretă implică un grad semnificativ de înșelăciune, pentru a ascunde identitatea organizatorului operației sau pentru a face să pară că o altă agenție ori entitate este implicată. Un exemplu cunoscut de astfel de operații este cel din luna mai 2007, atunci când ABC News și, mai târziu, The Daily Telegraph au afirmat că președintele Statelor Unite ale Americii George W. Bush a autorizat Agenția Centrală de Informații (CIA) să întreprindă „operații discrete" în Iran pentru a promova schimbarea regimului și pentru a sabota programul nuclear. Ulterior, ABC News a fost criticată pentru că a dezvăluit operația secretă, candidatul la președinția din 2008, Mitt Romney, declarând că a fost „șocat să vadă raportul ABC News privind

acțiunile secrete în Iran", dar ABC a spus că CIA și administrația George W. Bush știau de planurile lor, de a publica informațiile și nu au ridicat obiecții (Montopoli 2007). În luna iunie a aceluiași an, CIA a desecretizat o parte din documente și le-a făcut publice, în acestea detaliindu-se supravegherea ilegală, comploturi de asasinat, răpiri și alte operații „discrete", întreprinse în perioada anilor '50, '70, deoarece acestea ofereau o perspectivă asupra unei perioade foarte dificile și arăta profilul unei agenții de informații foarte diferit privind modul de acțiune pentru îndeplinirea sarcinilor.

O operație clandestină (clandestine operation) este o operație de informații sau militară, desfășurată în așa fel încât acțiunile și activitățile să fie neobservate de populația locală sau de structurile de informații și de contrainformații ale adversarului. Până în anii '70, operațiile clandestine au fost, în primul rând, de natură politică, vizate, în general, să sprijine grupuri sau națiuni pe care o altă entitate le favoriza. Exemplele includ implicarea serviciilor de informații americane cu criminali de război germani și japonezi după Cel de-Al Doilea Război Mondial sau acțiunea militară eșuată din Golful Porcilor din 1961. În prezent, aceste operații se regăsesc în metodele de acțiune ale multor structuri de informații de pe mapamond, sunt numeroase și se execută în funcție și de tehnologia avută la dispoziție.

Cea mai mare parte a operațiilor clandestine sunt legate de culegerea de informații, activitate desfășurată, de obicei, atât de către oameni, cât și de către senzori, amplasați în zone strategice sau camuflați în locuri importante. Amplasarea de cabluri de comunicații subacvatice sau terestre, de camere, microfoane, senzori de trafic, monitoare, precum snifferele, și de sisteme similare necesită ca misiunea să rămână nedetectată. Senzorii clandestini pot fi, de asemenea, montați pe vehicule subacvatice fără pilot, pe sateliți de cercetare, pe vehicule aeriene fără pilot (UAV) sau detectoare fără pilot, ori plasați manual de către surse umane clandestine.

Termenii clandestin și ascuns nu sunt sinonimi. După cum se menționează în definiție (care a fost folosită de Statele Unite și NATO încă din Cel de-Al Doilea Război Mondial), într-o operație sub acoperire, identitatea sponsorului este ascunsă, în timp ce într-o operație clandestină, operația în sine este ascunsă. Cu alte cuvinte, clandestin înseamnă „procedeu ascuns/stealth", atunci când se urmărește ca operația să nu fie descoperită. Termenul "stealth" se referă atât la un set larg de tactici, menite să ofere și să păstreze elementul surpriză, cât și la reducerea rezistenței inamicului la culegerea de informații. Ascuns înseamnă „să poată fi negat", astfel încât dacă operația este descoperită, aceasta să nu fie atribuită unui grup sau unei entități. Unele operații pot avea aspecte atât clandestine, cât și ascunse, cum ar fi utilizarea de senzori ascunși, amplasați la distanțe foarte mari sau de observatori umani, care sunt în măsură să direcționeze atacurile de artilerie și rachete terestre și loviturile acțiunilor aeriene. Atacul este evident, dar componenta folosită pentru a localiza ținta poate rămâne clandestină.

În Cel de-Al Doilea Război Mondial, țintele identificate și localizate prin criptoanaliza comunicațiilor radio au fost atacate doar dacă s-au executat și acțiuni

de cercetare aeriană a zonelor sau, în cazul doborârii avionului amiralului Isoroku Yamamoto, de observare, acțiune care a fost în sarcina Coastwatchers (Coast Watch Organization, Combined Field Intelligence Service, agenți aliați de informații militare, staționați pe insulele îndepărtate ale Pacificului). În timpul războiului din Vietnam, șoferii camioanelor atacate pe traseul Ho Chi Minh nu cunoșteau posibilitățile senzorilor deținuți de SUA, de tipul dispozitivului aeropurtat Black Crow, care identifica locația camioanelor după căldura motorului.

La acest moment, în Atanticul de Nord există o vastă infrastructură critică de rețele de cabluri submarine de comunicații între Europa și America de Nord, iar site-uri, precum TeleGeography, dețin hărți detaliate ale dispunerii cablurilor cu utilizări civile (energie, internet etc.), însă există și sisteme militare care nu fac obiectul unor asemenea postări, deoarece conțin date esențiale pentru toate formele de comunicare dintre membrii Alianței. Legat de aceasta, navele de cercetare electronică ale marinei ruse (de exemplu, nava Yantar, clasificată oficial ca navă auxiliară de cercetare generală oceanografică, cu capabilități de salvare subacvatică, care se subordonează unei structuri separate de marina militară a Ministerului rus al Apărării) acționează, uneori, pe ascuns (dezactivarea sistemului de identificare prin satelit), în apropierea cablurilor submarine vitale, determinând îngrijorarea oficialilor militari și de intelligence în legătură cu o eventuală interceptare a unor comunicări cu caracter secret.

O operație sub acoperire (covert operation) este o operație, executată de structurile militare sau de structurile de poliție, care implică un agent secret sau trupe care acționează sub o presupusă acoperire pentru a ascunde identitatea părții responsabile (Carson 2018). Conform legislației SUA, Agenția Centrală de Informații (CIA) este în măsură să conducă operații sub acoperire. Cadrul legislativ a definit acțiunea sub acoperire ca „activități speciale" atât politice, cât și militare, pe care guvernul SUA le poate refuza legal (Daugherty 2004). Efectul acestui cadru legislativ se regăsește într-o atenție deosebită pe care Congresul SUA o acordă CIA, în comparație cu celelalte structuri de informații.

Potrivit unui studiu, din 2018, al politologului, de la Universitatea din Chicago, Austin Carson, operațiile sub acoperire pot avea efectul benefic de a preveni escaladarea diferendelor în conflicte sau războaie. El susține că păstrarea secretului operațiilor militare poate limita dinamica escaladării, precum și izolarea liderilor de presiunile interne, permițându-le simultan să comunice adversarului interesul de a menține un război limitat (Carson 2018, 45).

Atunci când aceste operații sunt executate de structurile de poliție sintagma „sub acoperire" înseamnă a evita detectarea de către personalul monitor cu atribuții și mai ales a-și ascunde propria identitate (sau a folosi o identitate asumată), în scopul câștigării încrederii unui individ sau a unei organizații, pentru a afla ori a confirma informații confidențiale, ori pentru a câștiga încrederea persoanelor vizate în vederea culegerii de informații sau de dovezi. Operațiile sub acoperire, în mod tradițional, sunt executate de structurile de aplicare a legii, iar cei care îndeplinesc astfel de roluri sunt denumiți, în mod obișnuit, agenți sub acoperire.

Primele acțiuni au fost desfășurate în anul 1883 pe teritoriul Irlandei, au vizat combaterea acțiunilor de amplasare a bombelor pe care Frăția Republicană Irlandeză care le începuse cu câțiva ani mai devreme, iar agenții care au acționat au fost pentru prima dată instruiți în tehnici și tactici de combatere a terorismului. În 1906 pe teritoriul Statelor Unite a fost desfășurată o activitate similară, atunci când au fost înființate „echipele italiene" pentru a combate criminalitatea și a intimida elementele agresive din cartierele italiene sărace.

Există două probleme principale care pot afecta agenții sub acoperire. Prima este menținerea identității, iar a doua este reintegrarea în activitatea normală după îndeplinirea obiectivelor operației. A trăi o viață dublă într-un mediu nou prezintă multe probleme, deoarece munca sub acoperire este una dintre cele mai stresante activități pe care le poate întreprinde un agent special. Principala cauză a stresului este separarea agentului de prieteni, familie și de mediul său normal. Stilul de viață al agenților sub acoperire este foarte diferit de cel al polițiștilor obișnuiți și după încheierea misiunii, este dificil să se reintegreze în sarcinile cotidiene. După un astfel de stil de viață liber, agenții pot avea probleme de subordonare, de disciplină sau se simt inconfortabil și pot avea viziuni ciudate, uneori chiar paranoice despre lume și viață și pot fi permanent în stare de alertă.

De-a lungul istoriei, au fost desfășurate foarte multe operații de intelligence acoperite, care au avut ca scop obținerea de informații despre potențiali adversari, încă din perioada de pace. În acest context, se poate spune că astfel de operații fac parte din modul de acțiune al serviciilor de informații, în scopul avertizării timpurii a liderilor politico-militari (Piroșcă 2020, 2-3).

O operație sub steag fals (false flag) este un act comis cu intenția de a masca sursa reală a răspunderii și de a da vina pe o altă parte. Termenul a fost folosit pentru a descrie un truc în războiul naval prin care o navă arbora steagul unei țări neutre sau prietene pentru a-și ascunde adevărata identitate. Tactica a fost folosită, inițial, de pirați pentru a înșela alte nave, permițându-le astfel să se apropie de ele înainte de a le ataca. Mai târziu, a fost considerată o practică acceptabilă în timpul războiului naval, în conformitate cu legile maritime internaționale, cu condiția ca nava atacatoare să-și arate adevăratul pavilion, odată ce a început atacul (Ruis și Nilsson 2022, 18-35).

Astăzi, termenul mai reprezintă și organizarea de atacuri ale unor națiuni asupra lor, făcând ca acestea să pară a fi ale națiunilor inamice sau ale unor grupări teroriste, oferind astfel un pretext pentru represiune internă sau pentru declanșarea unei agresiuni militare. În acțiunile militare terestre, astfel de operații sunt, în general, considerate acceptabile în anumite circumstanțe, cum ar fi înșelarea inamicului, cu condiția ca înșelăciunea să nu fie perfidă și ca toate înșelăciunile să fie eliminate înainte de a deschide focul asupra inamicului.
Acest tip de operații de informații a fost utilizat ca pretext pentru declanșarea unor războaie. Astfel, incidentul Gleiwitz, din noaptea de 31 august 1939, l-a avut ca

protagonist pe Reinhard Heydrich, prin fabricarea dovezilor privind un atac polonez împotriva Germaniei, cu scopul de a mobiliza opinia publică germană la război și de a justifica războiul cu Polonia. Alfred Naujocks a fost un organizator cheie al operației, la ordinul lui Heydrich, care a dus la moartea câtorva deținuți din unele lagăre de concentrare naziste, care au fost îmbrăcați în soldați germani și apoi împușcați de Gestapo pentru a face să pară că au fost împușcați de soldații polonezi. Acest lucru, împreună cu alte operații sub steag fals din Operația Himmler, ar fi folosit pentru a mobiliza sprijinul populației germane pentru începutul Celui de-Al Doilea Război Mondial în Europa (Lightbody 2004). Operația nu a avut succes, deoarece nu a reușit să convingă opinia publică internațională de pretențiile germane, iar Marea Britanie și Franța au declarat război la două zile după ce Germania a invadat Polonia.

În februarie 2022, structuri de informații ale unor guverne occidentale au avertizat în legătură cu posibilitatea ca Federația Rusă să desfășoare o operație sub steag fals pentru a avea pretextul de a invada Ucraina. Aspectele premergătoare invaziei din 24 februarie au evidențiat o intensificare a campaniei de dezinformare și de inducere în eroare a Kremlinului și a mass-mediei ruse prin promovarea unor „steaguri false" aproape la fiecare oră, pretinzând că arată atacarea Rusiei de către forțele armate ucrainene, în încercarea de a justifica o invazie în Ucraina. Multe dintre videoclipurile postate pe canalele de socializare au fost pentru dezinformare, având o calitate slabă, metadatele nu s-au potrivit, deoarece au arătat date incorecte, iar dovezile și argumentele, prezentate de specialiștii de la Bellingcat și de alți jurnaliști independenți, au evidențiat că atacurile, exploziile și evacuările revendicate în Donbas au fost puse în scenă de Rusia.

În mod similar, în războiul naval o astfel de înșelăciune este permisă, cu condiția ca steagul fals să fie coborât și steagul adevărat să fie ridicat înainte de a se angaja în luptă (Squires 2008). Un exemplu notabil a fost crucișătorul german (fostă navă comercială) Kormoran, din Cel de-Al Doilea Război Mondial, care a surprins și a scufundat crucișătorul australian HMAS Sydney, în 1941, în timp ce era disimulat într-o navă comercială olandeză, provocând cele mai mari pierderi de vieți omenești pe o navă de război australiană. În timp ce Kormoran a fost grav avariat în timpul luptei și echipajul său a fost capturat, rezultatul a reprezentat o victorie morală considerabilă pentru germani.
În spionaj, termenul „steag fals" descrie recrutarea de agenți de către ofițerii de informații care se prezintă drept reprezentanți ai unei cauze față de care agenții potențiali îi simpatizează sau chiar propriul guvern al agenților.

Pentru a asigura succesul relațiilor internaționale ale unui stat și al operațiilor militare, factorii de decizie strategici trebuie să mai dispună și de măsurile necesare pentru a interzice posibilitatea adversarului de a executa acțiuni de terorism, spionaj, subversiune, sabotaj, crimă organizată sau de a ataca propriile rețele de comunicații și informatică. Pentru a realiza acest lucru, este necesară identificarea vulnerabilităților entităților proprii, iar rezultatele analizei vor fi trimise structurilor de contrainformații.

Contrainformațiile (CI) includ acele activități care se referă la identificarea și contracararea amenințării la adresa securității pe care o reprezintă serviciile sau organizațiile de informații ostile ori persoanele implicate în spionaj, sabotaj, subversiune sau terorism (NATO Standard AJP-2 2016; UK Ministry of Defence JP 2-00 2023), iar cea mai bună apărare împotriva atacurilor actorilor străini asupra teritoriului național, cetățenilor țării sau împotriva infiltrării serviciilor de informații constă în măsuri active și flexibile, cu posibilitatea de a alege cu rapiditate tehnicile de contrainformații, în funcție de evoluția situației, împotriva acelor servicii ostile, indiferent de apartenența lor. Această apărare este, de regulă, denumită contraspionaj, adică măsuri luate pentru a detecta spionajul inamicului sau atacurile fizice împotriva serviciilor de informații prietene, pentru a preveni deteriorarea și pierderea de informații și, acolo unde este posibil, pentru a întoarce tentativa împotriva inițiatorului său. Contraspionajul merge dincolo de a fi reactiv și încearcă în mod activ să submineze serviciul de informații ostil prin recrutarea de agenți în serviciul extern, prin discreditarea personalului efectiv loial propriului serviciu și prin luarea de resurse care ar fi utile serviciului ostil. Toate aceste acțiuni se aplică amenințărilor nonnaționale, precum și organizațiilor naționale.

Dacă acțiunea ostilă se desfășoară în propria țară sau într-una prietenă ori aliată, cu cooperarea structurilor de poliție, agenții ostili pot fi arestați sau, dacă sunt diplomați, declarați persona non grata. Din perspectiva unui serviciu de informații, exploatarea situației în avantajul părții este, de obicei, preferabilă arestării sau acțiunilor care ar putea duce la anihilarea amenințării. Prioritatea informațiilor intră, uneori, în conflict cu instinctele propriilor organizații de aplicare a legii, mai ales atunci când amenințarea străină combină personalul străin cu cetățenii țării.

În unele împrejurări, arestarea poate fi un prim pas în care deținutului i se oferă posibilitatea de a alege să coopereze sau să se confrunte cu consecințe grave până la condamnarea la moarte pentru spionaj. Cooperarea poate consta în a spune tot ce se știe despre celălalt serviciu, dar, de preferință, asistarea activă la acțiuni înșelătoare împotriva serviciului ostil.
Protecția serviciilor de informații se realizează prin organizarea contrainformațiilor defensive și implică evaluarea riscurilor asupra culturii, surselor, metodelor și resurselor acestora. Managementul riscurilor trebuie să reflecte în mod constant acele evaluări, deoarece operațiile eficiente de informații sunt adesea asumate de riscuri. Chiar și atunci când își asumă riscuri calculate, serviciile trebuie să atenueze riscul cu contramăsuri adecvate și, în mod special, pentru a descoperi metodele specifice artei schimbului de informații. Astăzi, serviciile de informații își dezvoltă capabilități pentru a explora alte entități de informații care se consideră deschise și pentru a putea submina persoane din interiorul comunității de informații. Contraspionajul ofensiv este cel mai puternic instrument de descoperire a intrușilor și de neutralizare a acestora, dar nu este singurul instrument.

În general, se subînțelege că guvernele se implică în acțiuni secrete (deoarece se implică în spionaj), acestea sunt de multe ori ilegale, conform legislației statului pe

teritoriul căruia se desfășoară. De asemenea, ele pot fi contrare legilor internaționale, la baza cărora stă principiul neamestecului în afacerile interne ale statelor suverane, deși acest principiu are din ce în ce mai multă greutate în jurisprudența internațională, după încheierea Războiului Rece (Shulski și Schmitt 2008).

Factorii de decizie au nevoie de informații care să nu fie controlate sau manipulate de forțe ostile. Deoarece fiecare disciplină de informații este supusă manipulării de către adversari, verdicitatea informațiilor și credibilitatea tuturor mijloacelor de culegere sunt esențiale. În consecință, fiecare organizație de contrainformații va valida fiabilitatea surselor și metodelor care se referă la misiunea de contrainformații, în conformitate cu standardele comune.

Atunci când o amenințare străină combină personalul străin cu cetățenii unei țări, avem de-a face cu operații de informații, sub denumirea de „coloana a cincea (fifth column)". În limbajul uzual, expresia îi desemnează pe cei care își trădează patria, care acţionează din interior, de obicei în favoarea unui grup inamic sau a unei alte naţiuni. De altfel, dicționarul Petit Robert definește sintagma prin „servicii secrete de spionaj inamice dintr-un teritoriu", iar Larousse, ca „element care lucrează pe un teritoriu în avantajul adversarului (sub această denumire au fost desemnaţi, în 1940, agenții serviciilor secrete germane care au acționat în Franţa)". Termenul se aplică și acțiunilor organizate de cadrele militare. Activitățile unei coloane a cincea pot fi la vedere sau clandestine. Toate persoanele și mijloacele materiale și financiare constituite în secret pot fi coordonate pentru a sprijini direct un atac din exteriorul țării. Activitățile clandestine, pentru o coloană a cincea, pot fi concretizate prin terorism, spionaj, sabotaj și dezinformare. Aceste acțiuni se execută exclusiv pe teritoriul național sau chiar în cadrul dispozitivului de luptă (pe timpul stărilor excepționale, instituite sau decretate) de către simpatizanții secreți ai unei forțe din afară.

Sintagma „coloana a cincea" își are originea în Spania (inițial quinta columna), datând din perioada premergătoare războiului civil spaniol. După cât se știe, a apărut, pentru prima dată, într-o telegramă secretă, din 30 septembrie 1936, trimisă la Berlin de către însărcinatul cu afaceri german la Alicante, Hans Hermann Völckers. În telegramă, el s-a referit la o „presupusă declarație a lui Franco" neidentificată, care se vehiculează (se pare că în zona republicană sau în zona levantină, deținută de republicani). Această „presupusă declarație" susținea că Franco a afirmat că existau patru coloane naționaliste care se apropiau de Madrid și o a cincea coloană care aștepta să atace din interior (termenul apare, pentru prima dată, într-o publicație spaniolă, după care, la 4 octombrie 1936, este preluată în publicația franceză *Le Journal*) (Le Journal 1936).

Public, termenul apare în numărul, din 3 octombrie 1936, al cotidianului comunist madrilen *Mundo Obrero*, iar până la jumătatea lunii octombrie, mass-media avertiza deja despre celebra coloană a cincea. Până la sfârșitul anilor '30, pe măsură ce implicarea americană în războiul din Europa a devenit mai probabilă, termenul de coloana a cincea a fost folosit în mod obișnuit pentru a avertiza despre potențiala

răzvrătire și neloialitate în interiorul granițelor SUA. Frica de trădare a fost sporită de căderea rapidă a Franței în 1940, pe care unii au pus-o pe seama slăbiciunii interne și a coloanei a cincea progermană, iar în Regatul Unit, într-un discurs adresat Camerei Comunelor, Winston Churchill i-a asigurat pe deputați că va acționa ca o mână de fier împotriva activităților coloanei a cincea.

Concluzii

Instrumentele de putere națională constau, de regulă, în ansambluri de surse de putere care trebuie să se adapteze permanent la schimbările care se petrec în mediul de securitate internațional sau chiar la cele din mediul intern al unui anumit stat. Instrumentul informațional este exercitat prin intermediul unor instituții specializate și are menirea de a furniza conducerii statelor, precum și celorlalte instituții care țin de alte instrumente de putere datele necesare adoptării celei mai potrivite decizii. Similar instrumentului diplomatic, instrumentul informațional este utilizat atât pe timp de pace, cât și în situații de criză sau în stare de război.
În acest sens, operațiile de informații sunt văzute de serviciile de informații ca metode și mijloace de folosire a agenturilor, de infiltrare a agenților în mediile de interes, din străinătate, în incursiuni pe teritoriul inamic, precum și în acțiuni de prevenire a unor acte de sabotaj sau de terorism pe teritoriul național.

Informațiile sunt vulnerabile nu numai la amenințările externe, ci și la cele interne. Trădarea și scurgerile de informații expun vulnerabilități, secrete guvernamentale și militare, surse și metode de informații. Amenințarea din interior este o sursă de daune extraordinare la adresa securității naționale, mai ales atuci când agenții au acces la informații referitoare la activități majore, discrete, sub acoperire sau clandestine.

Pentru planificarea, organizarea și desfășurarea operațiilor de informații, structurile de informații trebuie să își adapteze continuu activitățile la cerințele comandanților lor și la condițiile dure și des schimbătoare ale arenei informațiilor. Acest aspect implică în mod special agilitatea mentală și organizațională, susținută prin reziliență, adaptare și flexibilitate. Este normal ca succesul să apară mai târziu și de aceea este necesară perseverența în acțiuni, adaptarea rapidă și exploatarea oportunităților la momentul apariției lor. Pentru fiecare operație de informații, o agenție trebuie să elaboreze o metodologie specifică proiectului, asigurând astfel caracterul unic și complex al activităților, pentru a atinge scopul propus. Adaptarea rapidă a metodelor de lucru în domeniul informațiilor la mediul de acțiune și la ritmul de dezvoltare al tehnologiilor din domeniul informaticii și comunicațiilor obligă agenții secreți la o îmbunătățire a eficienței în culegerea informațiilor și la o flexibilitate a procedurilor de lucru, pentru a face față schimbării contextului și pentru a evita ideea că există doar o metodă de lucru.

La acest moment, putem spune că operațiile de informații sunt o acțiune uzuală care face parte din tacticile, tehnicile și procedurile de acțiune ale serviciilor de informații

din întreaga lume, în scopul cunoașterii permanente a intențiilor competitorilor sau ale statelor în care se manifestă ostilitate față de statul care inițiază astfel de operații, precum și pentru sprijinul acțiunilor militare și avertizării timpurii a liderilor politici și militari de la nivel strategic.

În concluzie, organizarea și desfășurarea operațiilor de informații în „Arena informațiilor" implică o rivalitate și o confruntare reală între serviciile de informații, pentru a câștiga unele avantaje în defavoarea celorlalte. Nu este surprinzător faptul că acești rivali încearcă permanent, pe de-o parte, să contracareze eforturile celuilalt de a-l cunoaște și, pe de altă parte, să-l inducă în eroare, să-l dezinformeze sau să-l înșele.

Referințe

Carson, Austin. 2018. *Secret Wars: Covert Conflict in International Politics.* Princeton University Press.

Daugherty, William J. 2004. *Executive Secrets: Covert Action and the Presidency.* University of Kentucky Press.

Evans, Tony și Peter H. Wilson. 1992. "Regime Theory and the English School of International Relations: A Comparison." *Millennium – Journal of International Studies* 21: 329 - 351.

Intelnews. 2008. "Tallinn government surveillance cameras reveal black bag operation." https://intelnews.org/2008/12/16/04-11/.

Le Journal. 1936. "La Passionaria prêche la terreur."

Lightbody, Bradley. 2004. *The Second World War: Ambitions to Nemesis.* Routledge.

Montopoli, Brian. 2007. "Știri CBS." http://www.cbsnews.com/8301-500486_162-2842625-500486.html.

Morgenthau, Hans J. 2007. *Politica între națiuni, Lupta pentru putere și lupta pentru pace.* Iași: Editura Polirom.

NATO AAP-6. 2021. "NATO Glossary of Terms and Definitions ."

NATO Standard AJP-2. 2016. "Allied Joint Doctrine for Intelligence, Counterintelligence and Security." Edition A Version 2. https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf.

Piroșcă, Valerică. 2020. „Operații de intelligence." *Colocviu Strategic* 6 (173): 2-3. https://cssas.unap.ro/ro/pdf_publicatii/cs06-20.pdf.

Ruis, Carlos Diaz și Tomas Nilsson. 2022. "Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies." *Journal of Public Policy & Marketing* (no. 42): 18-35.

Shulski, Abram N. și Gary J. Schmitt. 2008. *Războiul tăcut.* București: Editura Polirom.

Smith Jr., W. Thomas. 2003. *Encyclopedia of the Central Intelligence Agency.* New York: Facts on File Inc.

Squires, Nick. 2008. *HMAS Sydney found off Australia's west coast.* https://www.telegraph.co.uk/news/worldnews/australiaandthepacific/australia/1581972/HMAS-Sydney-found-off-Australias-west-coast.html.

U.S. Air Force Doctrine. 2023. "Air Force Doctrine Publication 2-0 - Intelligence." https://www.doctrine.af.mil/Doctrine-Publications/AFDP-2-0-Intelligence/.

UK Ministry of Defence JP 2-00. 2023. "Joint Doctrine Publication. Intelligence, Counter-intelligence and Security Support to Joint Operations." https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

Westwood, James T. 1977. "A contemporary political dilemma: the impact of intelligence operations on foreign policy." *Naval War College Review* 29 (4): 86-92. https://www.jstor.org/stable/44641751.